



Components of Biosecurity



Biosecurity Inspector Training

Staten Serums Institut

31 August – 2 September 2009

www.biosecurity.sandia.gov

SAND No. 2009-5485C

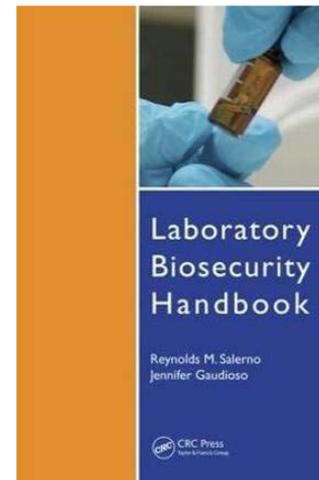
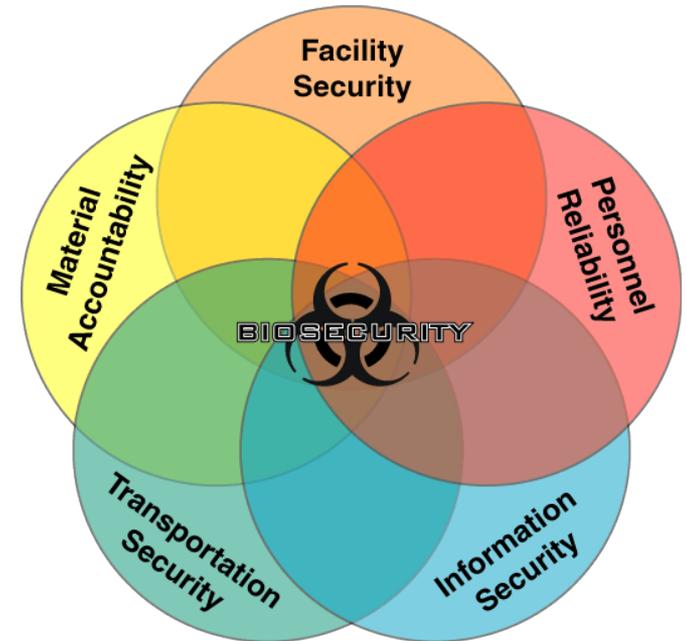
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

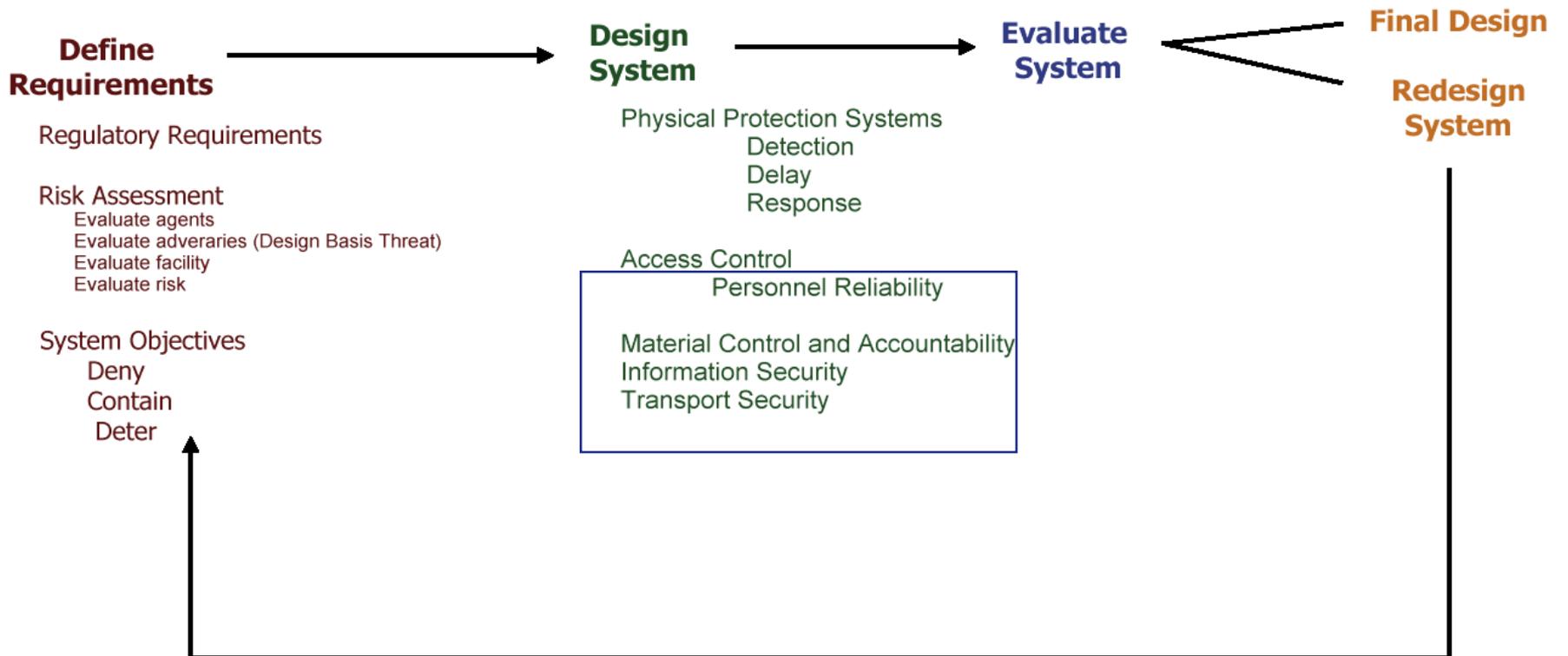




Biosecurity Systems – A Comprehensive Approach

- Biosecurity system components
 - Physical security
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices
- Each component implemented based on results of risk assessment







“Somebody once said that in looking for people to hire, you look for three qualities: integrity, intelligence, and energy. And if they don't have the first, the other two will kill you. You think about it; it's true. If you hire somebody without the first, you really want them to be dumb and lazy.”

- Warren Buffett



Personnel Reliability

- The objectives of a personnel reliability program are to
 - Help to judge a person's integrity
 - E.g. reduce the risk of theft or fraud
 - E.g. reduce the risk of scientific misconduct
 - To support the procedural and administrative access control requirements
 - To support the biosafety program





Which Personnel to Vet?

- **Insiders**
 - Have authorized access to the facility, dangerous pathogens, and/or restricted information
 - The insider depends on a facility's access controls and visitor controls
- **Not all positions present the same risk**
 - Consider the potential consequences
 - Consider not just the researchers but those also with access like the security force, system/network administrators, locksmith, etc.



Approaches for Vetting Individuals

- Public records
 - Use may be governed by local or national regulations
- Interviews
- Personality testing
- Skill testing
- Drug testing
- Considerations
 - Accuracy of information obtained during vetting process
 - Have applicant sign “release of information” statement
 - If periodic reinvestigations will be required, notify applicant during hiring process
 - Legal constraints on use of information for employment decisions





National Checks

- Individual's can obtain a National Police Criminal History Record
 - E.g. FBI Identification Record
- Institutions can pay commercial investigators to conduct background screening on potential/current employees
- Institutions can run background checks using publically accessible information
 - Educational Records
 - Profession Credentials
 - Military Records
 - Court Records
 - Criminal Checks
 - Financial Checks





Reinvestigations

- A security reinvestigation establishes any security related changes in a person's life
 - The same checks are typically run as in initial investigation
 - Timeline from last investigation to present
 - Identifies changes like
 - New personal contacts
 - New financial situations
 - Situations which should have been reported
 - Discrepancies from past investigations
- Federal Requirements
 - Select agent
 - Reinvestigation every 5 years





Background Screening Discussion

- Should individuals working in all areas of a bioscience facility require the same level of screening?
- Which individuals are not currently screened?
- Is the current background screening process sufficient for those working with biological agents?
- Are screening process sufficient for visitors? What about long-term visitors from a foreign country?



In-Processing

- Program should document the steps necessary prior to granting an individual authorized access, e.g.
 - Background investigation
 - Safety and security training
 - Job –specific briefing
 - Immunizations
- Where do new hires work until vetting process and trainings are complete?
 - Can take months to years depending on process





Out-Processing

- Change access
 - Do combination locks need to be changed?
- Retrieve property, including
 - Badges, keys
 - Laboratory notebooks
 - Pathogenic materials
 - Laptops, PDAs, cell phones, pagers
 - Library materials
- Deactivate computer and electronic access accounts
- If appropriate, notification of Responsible Official to change Select Agent program registration





Badges

- Badges should be issued to those individuals authorized to be in restricted areas
- Badge information should include
 - Individual's name
 - Individual's photograph
 - Expiration date
 - Indication of areas where individual has authorized access
- Badge return
 - Upon employee termination
 - Daily or at the conclusion of a limited term for visitors
- Report lost or stolen badges

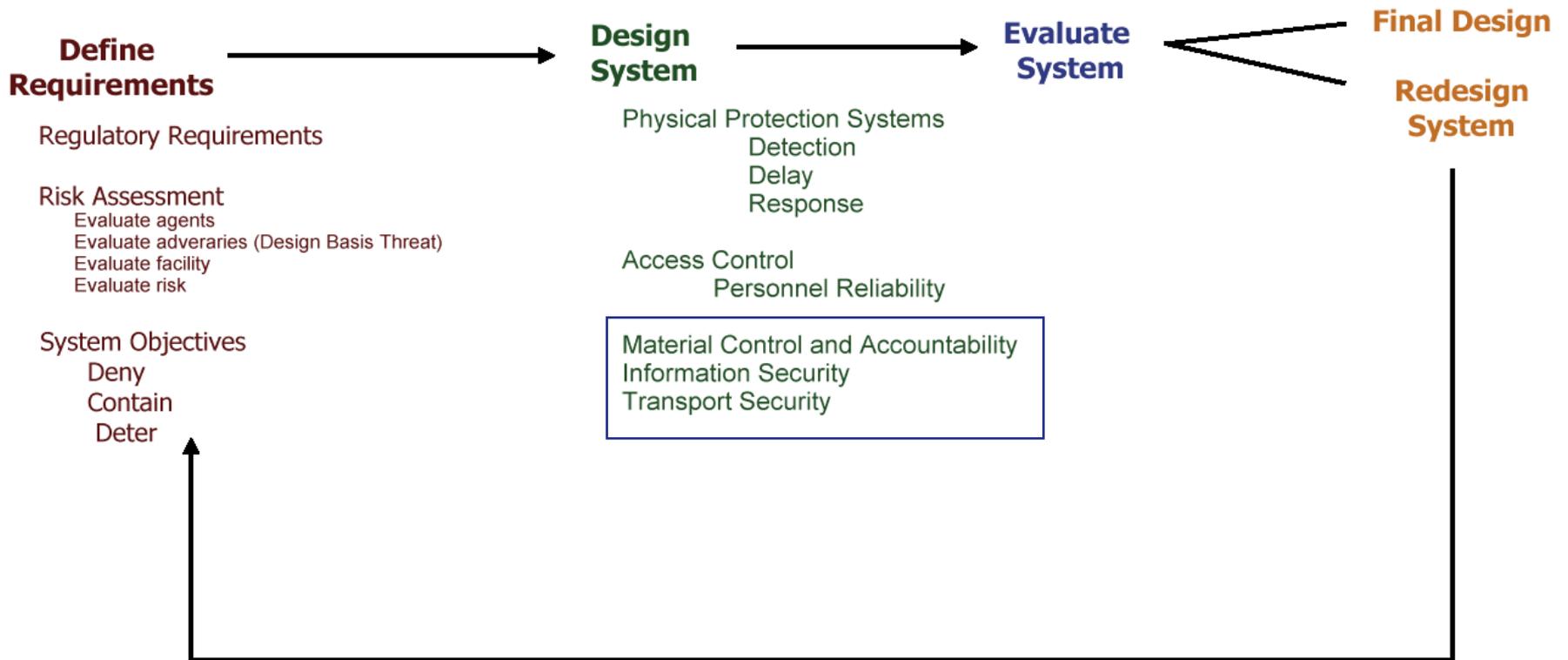




Visitor Controls

- Types
 - Personal Visitors
 - Family members
 - Casual Visitors
 - Tours, seminars
 - Equipment repair technicians
 - Working Visitors
 - Visiting researchers
 - Facility maintenance personnel
- Controls
 - All visitors should have a host at the facility
 - Visitors should be escorted in restricted areas
 - Institution needs to establish policy on amount advance notice required for each type of visitor





Material Control and Accountability

- Material Control and Accountability (MC&A) ensure complete and timely knowledge of:
 - **What materials exist**
 - **Where the materials are**
 - **Who is accountable for them**
- NOT: to detect whether something is missing



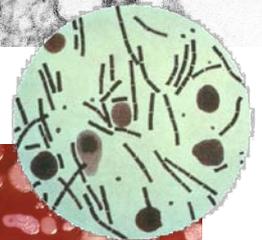
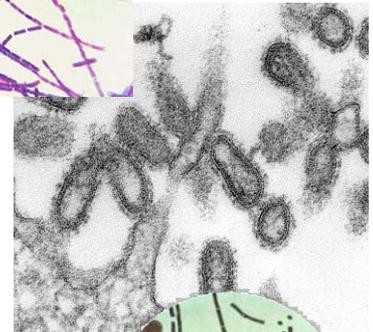
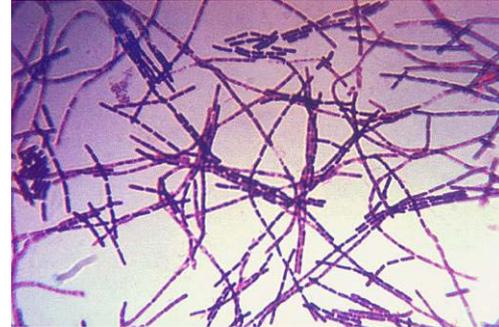


Material Control and Accountability Discussion

- What are some of the reasons you think a bioscience facility should implement MC&A besides for biosecurity?
- What details should be in a laboratory inventory and are they feasible with biological agents? Is it ever appropriate for the facility and laboratory have different levels of detail in their inventories?
- What is the span of the MC&A program? (E.g. from a blood sample submitted for diagnosis until the sample and all other items used in diagnosis destroyed?)
- What documentation should be kept on day to day use, repositories, destruction?
- Are there any information security concerns about MC&A information?

Material Control and Accountability

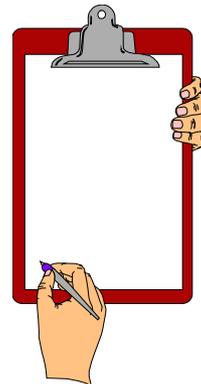
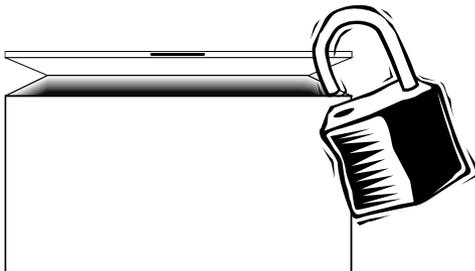
- Agent
 - What agents are high risk?
 - Viable? Whole organism or DNA?
- Quantity
 - Any amount can be significant
 - A threshold amount for toxins
- Form
 - Repository stocks, working samples, in host, contamination
- Detail—what level is adequate for MC&A?
 - Material as *items*
 - Each vial as a separate inventory record?
- Capture—when does MC&A start & stop?
 - Naturally occurring; clinical samples; disposition





Material Control and Accountability

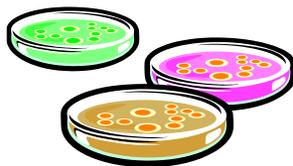
- Control is either...
 - Engineered / Physical
 - Administrative
- Containment is part of material control
 - Containment Lab / Freezer / Ampoule
- Procedures are essential for material control
 - For both normal and abnormal conditions





Material Control and Accountability

- All material should have an associated “accountable person”
 - The person best in a position to answer questions about the associated material
 - Not someone to blame!
 - Ensure that no material is “orphaned”
- Procedures should ensure accountability
 - Experimental work: laboratory procedures
 - Inventory: know what you have
 - Reporting: document routine MC&A practices
 - Audit/ assessment: is this working?
 - Ensures effective *implementation* of MC&A
 - Training: personnel understand requirements





Material Control & Accountability Examples

- Moderate risk biological agents
 - Seed stocks cataloged and records stored securely
 - Transfers in and out
 - Source
 - Strain
 - Form
 - Responsible individual
 - Working stocks, including infected animal status, tracked through laboratory notebooks
- High risk biological agents
 - Moderate plus
 - Increased control over working stocks





Information Security Discussion

- What information at a bioscience institution should not be disclosed to the public?

- Should all employees at an institution have access to all information? Why or why not? If not, what information should be limited access, even for internal distribution?



Information Security

- Protect information that is too sensitive for public distribution
- Risks to information include
 - Loss of integrity
 - Loss of confidentiality
 - Loss of availability
- Biosecurity-related sensitive information
 - Security of dangerous pathogens and toxins
 - E.g. Risk assessments
 - E.g. Security system design
 - Access authorizations





Information Security: Identification, Control, and Marking

- Identification
 - Designated sensitivity level
 - A review and approval process aids in the identification of sensitivities
 - Critical prior to public release of information
- Control
 - Individual responsible for control of sensitive information
 - Physical security
 - Communication security
 - In the US, in order to refuse public access upon request, information must be exempt from the Freedom of Information Act
- Marking
 - Sensitivity level designation
 - Top and bottom of each page / cover sheet
 - Marking and control methods should be well understood by those working with information

Moderate

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20008

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for
Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

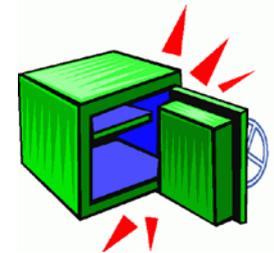
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration

Declassify on: December 31, 2000

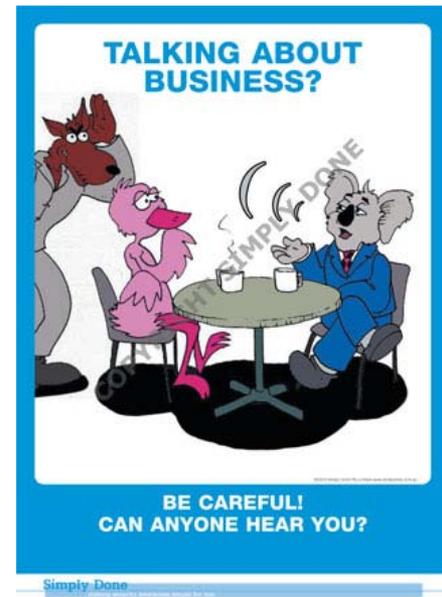
Moderate





Information Security: Communication and Network Security

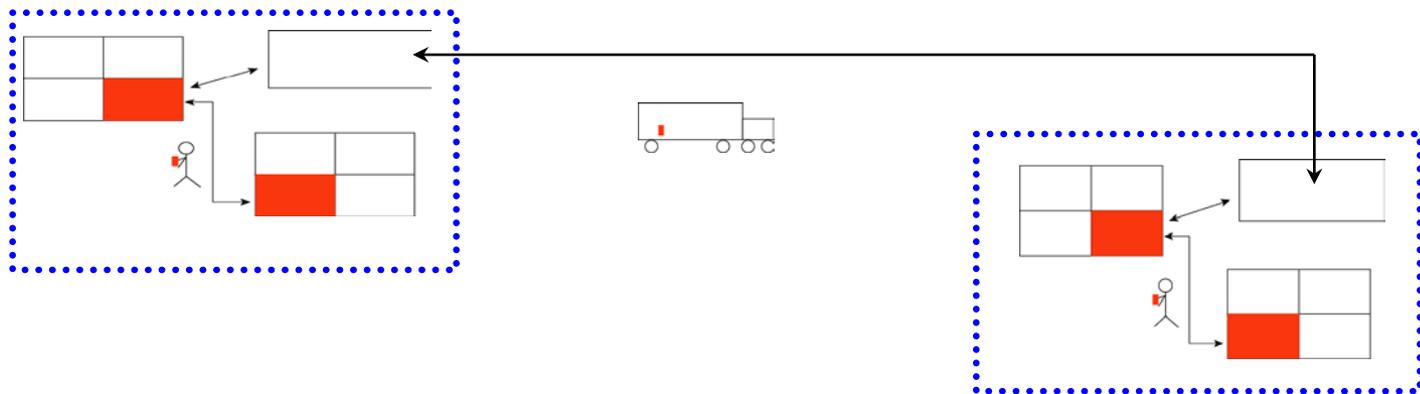
- Communication Security
 - Mail, email, or fax security is required
 - Limited discussions in open areas
 - Information should only be reproduced when needed and each copy must be controlled as the original
- Network Security
 - Firewalls
 - User authentication
 - Virus protection
 - Layered network access
 - Desktop security
 - Remote and wireless access controls
 - Encryption
 - Authentication





Infectious Substance Transport

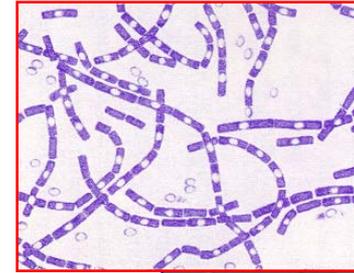
- Transport – movement of biological material outside of a restricted area
- Transport can occur
 - Across international borders
 - Within a country
 - Within a facility
- Protection while in transport should be comparable that in the restricted area
 - May require a documented chain of control



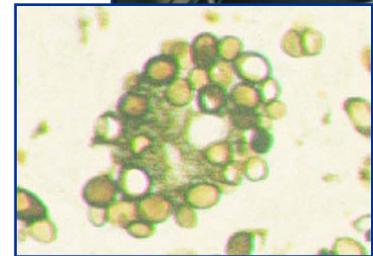
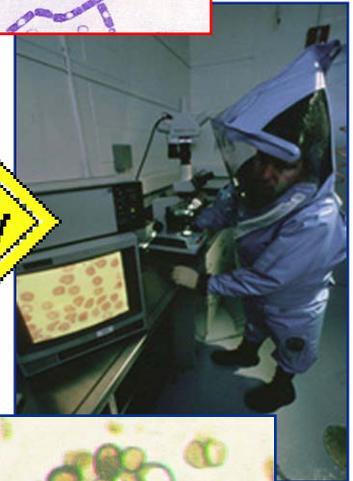


Transportation Security

- Infectious substances (Class 6.2) and toxins (Class 6.1) are defined as Dangerous Goods
- Transportation security include:
 - Training
 - Security awareness training
 - Specific training as appropriate
 - Written security plan
 - Based on assessment of transportation security risks
 - Address personnel security, unauthorized access, en route security



Bacillus anthracis





External Transport

- Movement of materials from one facility to another facility
- May involve commercial carriers
- Occur within a wide array of international and state regulations and standards
- Must be able to move frozen materials efficiently
- Needs to be cost-effective





Transport Security Discussion

- What level elements of transport security should be implemented for internal facility transport of the following biological agents?
 - Non-infectious bacteria (*E-coli K12*)
 - Multi-drug resistant strain of *M. tuberculosis*
 - Frozen vial containing the Spanish Flu (1918 Influenza strain)
- What measures would you add for external transport for the same biological agents?



Transport Security: Facility Responsibilities

- Personnel security
 - For people who have access to dangerous pathogens and toxins or information during transfers
- Establish chain of custody (CoC)
 - Record all individuals who have contact with the dangerous pathogens and toxins
- Provide physical security
 - For packages that need temporary storage
- Protect transport documentation
- Determine who is able to authorize, transport, and receive dangerous pathogens and toxins



Carrier Security

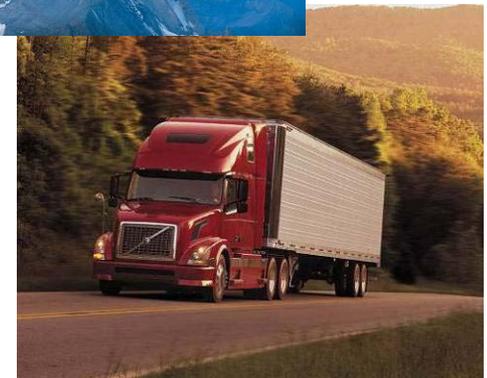
- Carriers should provide security by
 - Ensuring reliable and trustworthy people handle the package
 - Controlling access to transport facilities, docks, and vehicles
 - Tracking shipping progress
 - Providing ongoing security training for employees





Transport Security

- Moderate risk agents
 - Internal transport personnel screened
 - Recipient screened for legitimacy
 - Safe receipt notification
- High risk agents
 - Moderate plus
 - Chain of custody
 - Physical controls on storage containers





Define Requirements

Regulatory Requirements

Risk Assessment

Evaluate agents
Evaluate adversaries (Design Basis Threat)
Evaluate facility
Evaluate risk

System Objectives

Deny
Contain
Deter

Design System

Physical Protection Systems
Detection
Delay
Response

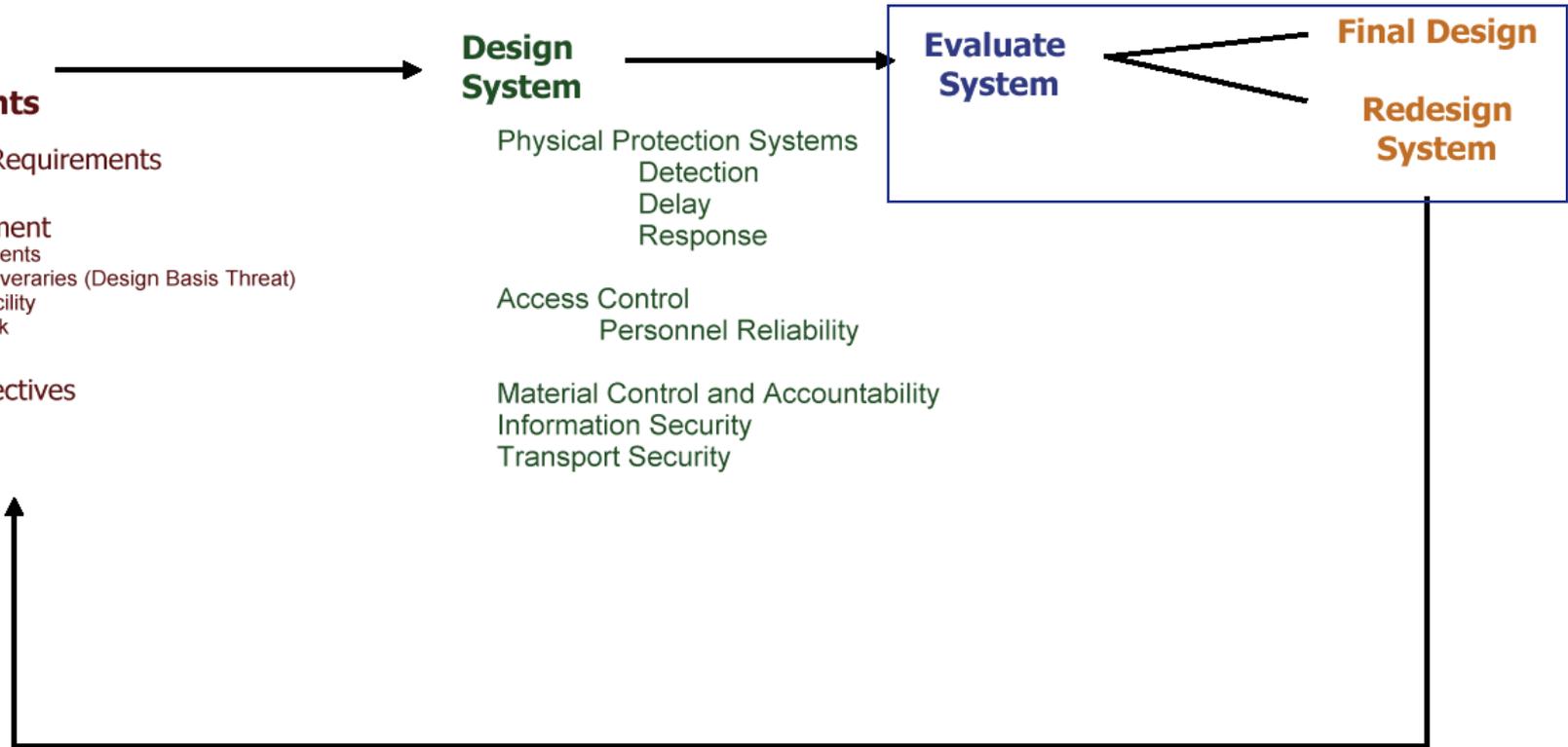
Access Control
Personnel Reliability

Material Control and Accountability
Information Security
Transport Security

Evaluate System

Final Design

Redesign System





Security Violations Discussion

- What are some examples of security violations?
- How could they be prevented?
- How should management deal with security violations?





Components of Biosecurity

